



Karen Zacharia
Chief Privacy Officer

1300 I Street, NW, Suite 500 East
Washington, DC 20005
Phone 202.515.2529
Fax 202.336.7923
karen.zacharia@verizon.com

April 5, 2019

Hon. Ron Wyden
U.S. Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Wyden:

I write in response to your March 13, 2019 letter to Hans Vestberg, Chief Executive Officer of Verizon. In our prior letters to you, we detailed how we terminated our location aggregator program when we learned that the program was the subject of misuse. Our protection of customer location data, however, does not end there. Verizon uses a myriad of methods to protect our customers' information, including location information, from the always evolving threat of fraudsters and criminals.

Verizon, like the other carriers to whom you sent letters, regularly receives warrants from law enforcement seeking location information. Verizon and the other carriers also regularly receive requests from law enforcement and other government agencies for location information in emergencies involving the danger of death or serious physical injury. These emergency requests may be made in response to active violent crimes – such as bomb threats, hostage situations, kidnappings and fugitive scenarios – or in search and rescue settings, including when governmental entities are trying to locate a missing child or elderly person.

Numerous lives have been saved through Verizon's and other wireless carriers' assistance to law enforcement in responding to these emergencies. For example, a woman was found safe last year after her car got stuck in the snow southeast of Ukiah, Oregon when she was en route from Portland to Boise.¹ Her rescue was made possible because Verizon provided location information regarding the woman's cell phone (*i.e.*, the cell site closest to her phone) to the Oregon State Police. And this is not an outlier example. Just last month, location information provided by Verizon helped a county Sheriff's office find an elderly Oregonian with dementia. Indeed, many people have been saved over the years because of information provided by carriers to law enforcement quickly in response to emergency situations.

¹ <https://www.kgw.com/article/news/local/missing/woman-found-safe-after-car-gets-stuck-in-snow-on-way-to-boise/283-509845122>.

Even in these urgent, time-sensitive situations, Verizon takes reasonable and responsible efforts to protect our customers' information. Before sharing information with law enforcement, Verizon performs several actions to confirm the law enforcement individual is who they claim to be. In so doing, Verizon has caught pretexters falsely posing as law enforcement. And as fraudsters' techniques evolve, Verizon adapts our confirmation process as well. Fraudsters who abuse—or attempt to abuse—this process are criminals and should be prosecuted to the fullest extent of the law. We thus work not only to prevent fraudsters from improperly gaining access to customer information, but we also work with law enforcement to identify and prosecute them. And, although Verizon was not involved in the case, we understand that the fraudster identified in the March 6 Motherboard article was arrested and served time in prison for impersonating a law enforcement officer.

Finally, Verizon reports breaches of Customer Proprietary Network Information to the United States Secret Service ("USSS") and Federal Bureau of Investigation ("FBI") through the FCC's Data Breach Reporting Portal as required by law. We also regularly work directly with the USSS, FBI, and other law enforcement agencies to identify and prosecute individuals when our customers' information is unlawfully obtained.

We are committed to protecting the privacy and security of our wireless subscribers' location information. We recognize that location information can provide many pro-consumer benefits but we must protect that data from unauthorized access and use. Our subscribers' trust and comfort surrounding the use of location information will remain paramount, and we plan to act accordingly.

Sincerely,

A handwritten signature in blue ink, appearing to read "Karen Zacharia", is written over a horizontal line.

Karen Zacharia
Chief Privacy Officer
Verizon

1300 I Street, NW – Suite 500 East
Washington, D.C. 20005